p-adic properties of division polynomials and elliptic divisibility sequences

JOSEPH H. SILVERMAN

ABSTRACT. For a fixed rational point $P \in E(K)$ on an elliptic curve, we consider the sequence of values $\big(F_n(P)\big)_{n\ge1}$ of the division polynomials of E at P. For a finite field $K/\mathbb{F}_p$, we prove that the sequence is periodic. For a local field $K/\mathbb{Q}_p$, we prove (under certain hypotheses) that there is a power $q = p^e$ so that for all $m \ge 1$, the limit of $F_{mq^k}(P)$ as $k \to \infty$ exists in K and is algebraic over $\mathbb{Q}(E)$. We apply this result to prove an analogous p-adic limit and algebraicity result for elliptic divisibility sequences.

CONTENTS

Date: April 2004.

1991 *Mathematics Subject Classification.* Primary: 11G07; Secondary: 11D61, 14G20, 14H52.

Key words and phrases. elliptic curve, division polynomial, elliptic divisibility sequence.

The author's research supported by NSA grant H98230-04-1-0064.

Introduction

Let E/K be an elliptic curve given by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

and let $z = -x/y$ be the usual uniformizer at $\mathcal{O}$. The n-division polynomial F_n of E is the function $F_n \in K[x, y] \subset K(E)$ with divisor

$$(F_n) = [n]^*(\mathcal{O}) - n^2(\mathcal{O}),$$

suitably normalized at $\mathcal{O}$ (see Definition 1). Division polynomials play for elliptic curves the role that is played by the polynomials $X^n - 1$ for the multiplicative group.

Complex analytically the n-division polynomial of an elliptic curve $\mathbb{C}/L$ is equal to the quotient $\sigma(n\zeta, L)/\sigma(\zeta, L)^{n^2}$ of Weierstrass σ-functions [26, Chapter XX, Misc. examples 24 and 33]. Division polynomials play a prominent role in the theory of elliptic functions and elliptic curves, appearing in the elliiptic addition law, in the theory of complex multiplication, in transformation formulas for canonical local heights, in the theory of elliptic divisibility sequences, and in the cryptographically important SEA algorithm of Schoof, Elkies, and Atkins [15, 16] for counting points on elliptic curves over $\mathbb{F}_p$.

In this paper we study the sequence of values $(F_n(P))_{n\ge1}$ of the division polynomials evaluated at a point $P \in E(K)$. We will be especially interested in periodicity properties when K is a finite ring or finite field and in convergence properties when K is a complete local field. We now describe special cases of our three main theorems for $\mathbb{F}_p$, $\mathbb{Z}/p^\mu\mathbb{Z}$, and $\mathbb{Q}_p$. See Corollary 9, Theorem 12, and Theorem 14 for general statements.

Theorem 1. *Let $E/\mathbb{F}_p$ be an elliptic curve and let $P \in E(\mathbb{F}_p)$ be a point of exact order $r \ge 2$. Then the sequence $(F_n(P))_{n\ge0}$ is periodic with period rt for some integer t dividing $p - 1$ if $r \ge 3$ and dividing $2p - 2$ if $r = 2$.*

Our proof of Theorem 1, which is modeled after a similar result by Ward [24, Theorems 8.1 and 9.2] for elliptic divisibility sequences, proceeds by first lifting to a field of characteristic 0 and then embedding the problem into $\mathbb{C}$ and using the transformation law for the Weierstrass σ-function.

Theorem 2. *Let $E/\mathbb{Q}_p$ be an elliptic curve with good ordinary reduction, let $P \in E(\mathbb{Q}_p)$ be a point whose reduction modulo p has order r, and let rt be the period of the sequence $(F_n(P))_{n\ge0}$ (cf. Theorem 1).*

Assume further that $p \geq 3$, that $r \geq 3$, and that $p \nmid r$. Fix a power p^e of p satisfying $p^e \equiv 1 \pmod{rt}$. Then for every $m \geq 1$, the limit

$$G_m(P) := \lim_{k\to\infty} F_{mp^{ek}}(P) \quad \text{converges in } \mathbb{Z}_p.$$

Further, $G_m(P) = 0$ if and only if $r|m$.

If in addition E is defined over $\mathbb{Q}$ and $P \in E(\mathbb{Q})$, then $G_m(P)$ is algebraic over $\mathbb{Q}$.

The proof of Theorem 2 uses the Mazur-Tate p-adic σ-function [12], which is why the statement of the theorem is restricted to the case of curves with ordinary reduction. However, it is likely that the statement is true in general. We will use similar techniques to prove the following periodicity result modulo higher powers of p. (See Remark 4.) This may be compared with Shipsey [19, Theorem 3.5.4], who uses explicit formulas to prove an analogous result for elliptic divisibility sequences modulo p^2.

Theorem 3. *With notation and assumptions as in Theorem 2, for every $\mu \geq 1$, the sequence*

$$\big(F_{kr}(P) \bmod p^\mu\big)_{k\geq 1}$$

is periodic with period dividing $p^{\mu-1}(p-1)$.

As an application of Theorem 2, we will partially answer a question raised in [22] concerning elliptic divisibility sequences. A (proper) *elliptic divisibility sequence* is a sequence $\mathcal{W} = (W_n)_{n\geq 0}$ of integers whose initial terms satisfy $W_0 = 0$, $W_1 = 1$, $W_2W_3 \neq 0$, $W_2|W_4$, and whose subsequent terms are determined by the nonlinear recursion

$$W_{m+n}W_{m-n} = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2$$

for all $m \geq n \geq 1$. Ward, who made an extensive study of these sequences [24, 25], shows that a proper elliptic divisibility sequence $\mathcal{W}$ is associated to a (possibly singular) elliptic curve $E_{\mathcal{W}}$ and point $P_{\mathcal{W}} \in E_{\mathcal{W}}(\mathbb{Q})$ and that the values of W_n are closely related to the values of the division polynomials $F_n(P_{\mathcal{W}})$. More recently, elliptic divisibility sequences have been studied by Shipsey [19], who gives an application to the elliptic curve discrete logarithm problem, and by several other authors [3, 4, 5, 8, 9, 10, 23, 22]. (See also [11, 13, 14] for work on the related Somos sequences.)

In [22], Nelson Stephens and the author proved that for any fixed modulus 2^e, the sequence

$$(W_{2^k} \bmod 2^e)_{k\geq 0}$$

is eventually periodic, and the question was raised as to whether this periodicity reflects a subtler p-adic convergence property. In this paper we use the results cited above to prove p-adic convergence for almost all primes.

Theorem 4. *Let $\mathcal{W} = (W_n)_{n\ge 0}$ be a proper elliptic divisibility sequence, and assume that the associated elliptic curve $E_{\mathcal{W}}$ is nonsingular and does not have complex multiplication. Then for almost all primes p, in the sense of density, the following two statements are true.*

(a) *There is an exponent $N = N_p \ge 1$ so that for every $m \ge 1$, the limit*

$$\lim_{k\to\infty} W_{mp^{k\tau}} \quad \text{converges in } \mathbb{Z}_p. \tag{1}$$

(b) *The limit given by (1) is algebraic over $\mathbb{Q}$.*

(If $E_{\mathcal{W}}$ has complex multiplication, then (a) and (b) are true for at least half of all primes, more precisely, they are true for all but finitely many of the primes that split in the CM field of $E_{\mathcal{W}}$.)

Although we are only able to prove Theorem 4 for almost all primes, we see no reason why it should not be true in general.

Conjecture 5. *Statements* (a) *and* (b) *of Theorem 4 are true for every proper elliptic divisibility sequence and for every prime p.*

In our proof of Theorem 4, it is natural to avoid a certain finite set of primes at which (W_n) behaves badly. However, the reason that we ultimately eliminate infinitely many primes is because we used the Mazur-Tate p-adic σ-function [12] in our proof of Theorem 2, so that theorem only applies to elliptic curves with ordinary reduction. A theorem of Serre [17] says that for a fixed (non-CM) elliptic curve $E/\mathbb{Q}$, almost all primes are ordinary, but since Elkies [6] has shown that there are also infinitely many primes of supersingular reduction [6], our proof cannot be directly extended to prove Theorem 4 for all but finitely many primes.

1. Elliptic curves and division polynomials

Let E/K be an elliptic curve defined over any field K, and fix a Weierstrass equation for E,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then $z = -x/y \in K(E)$ is a uniformizer at $\mathcal{O} \in E$, and the invariant differential $\omega = dx/(2y + a_1x + a_3)$ can be expanded as a formal (Laurant) series in a formal neighborhood of $\mathcal{O}$ as

$$\omega(z) = (1 + a_1z + (a_1^2 + a_2)z^2 + \cdots)\,dz.$$

This series has coefficients in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$, and we have normalized matters so that $(\omega/dz)(\mathcal{O}) = 1$.

Definition 1. Let $n \geq 1$ be an integer and let $[n](z) \in K[[z]]$ be the power series defining the multiplication-by-n map on the formal group of E. The *n-division polynomial* F_n (normalized relative to the uniformizer z) is the unique rational function $F_n \in K(E)$ satisfying

$$(F_n) = [n]^*(\mathcal{O}) - n^2(\mathcal{O}) \quad \text{and} \quad \left(\frac{z^{n^2} F_n}{[n](z)}\right)(\mathcal{O}) = 1.$$

If $n \neq 0$ in K, then $[n](z) = nz + O(z^2)$, so the normalization condition becomes simply $(z^{n^2-1} F_n)(\mathcal{O}) = n$. (For a more general normalization procedure, see Remark 1.)

We will use the following elementary "chain rule" for division polynomials.

Lemma 6. *For all integers $m, n \geq 1$,*

$$F_{mn} = \big(F_n \circ [m]\big) \circ F_m^{n^2}.$$

Proof. It is an easy exercise to verify that both sides have the same divisor and the same leading term at $\mathcal{O}$. Or see [12, Appendix I, Proposition 4] for a more general version. □

2. Divison polynomials over $\mathbb{C}$ and the Weierstrass σ-function

Let $E/\mathbb{C}$ be an elliptic curve and fix an isomorphism $\Phi : \mathbb{C}/L \to E(\mathbb{C})$ with a lattice $L \subset \mathbb{C}$. The classical n-division function on $\mathbb{C}/L$ is

$$\psi_n(\zeta, L) = \frac{\sigma(n\zeta, L)}{\sigma(\zeta, L)^{n^2}},$$

where $\sigma(\zeta, L)$ is the Weierstrass σ-function. We check that with the given normalization of F_n, the relationship between F_n and ψ_n behaves consistantly with respect to n.

Lemma 7. *Let $E/\mathbb{C}$ be an elliptic curve and $\Phi : \mathbb{C}/L \to E(\mathbb{C})$ an isomorphism as above. Then there is a constant $\gamma \in \mathbb{C}^*$ so that*

$$F_n(\Phi(\zeta)) = \gamma^{1-n^2} \psi_n(\zeta, L) \qquad \textit{for all } \zeta \in \mathbb{C} \textit{ and all } n \geq 1.$$

Proof. The analytic n-division function $\psi_n(\zeta, L)$ on $\mathbb{C}/L$ has the same divisor as $F_n \circ \Phi$, so they are constant multiples of one another,

$$F_n(\Phi(\zeta)) = c_n \psi_n(\zeta, L) \qquad \text{for all } \zeta \in \mathbb{C}. \tag{2}$$

The Weierstrass σ-function satisfies $\sigma(\zeta,L)=\zeta+O(\zeta^2)$ as $\zeta\to 0$, so $\psi_n(\zeta,L)=(n/\zeta^{n^2-1})\bigl(1+O(\zeta)\bigr)$. The map Φ has the form $(z\circ\Phi)(\zeta)=\gamma\zeta+O(\zeta^2)$ in a neighborhood of 0, since Φ is an isomorphism and ζ and z are, respectively, uniformizers in neighborhoods of 0 and $\mathcal{O}=\Phi(0)$. Hence

$$F_n(\Phi(\zeta))=F_n\bigl(\gamma\zeta+O(\zeta^2)\bigr)=\frac{n}{(\gamma\zeta)^{n^2-1}}\bigl(1+O(\zeta)\bigr)=\gamma^{1-n^2}\psi_n(\zeta,L).$$

Comparing this with (2), we see that with our chosen normalization of F_n, there is a single constant $\gamma\in\mathbb{C}^*$ such that

$$F_n\circ\Phi=\gamma^{1-n^2}\psi_n\qquad\text{for all } n\ge 1. \qquad\square$$

3. Periodicity of division polynomials over finite fields

In this section we prove that the values of division polynomials over finite fields form a purely periodic sequence. Our proof is modeled after an analogous result by Ward (especially [24, Theorems 8.1 and 9.2]) for elliptic divisibility sequences. The proof uses a lift to characteristic zero and the Lefschetz principle. It would be interesting to find a purely finite field proof.

Theorem 8. *Let $\mathbb{F}$ be a finite field, let $E/\mathbb{F}$ be an elliptic curve, and let $P\in E(\mathbb{F})$ be a point of exact order $r\ge 2$. Then there are units $a,b\in\mathbb{F}^*$, depending on P, such that:*

(a) *If $r\ge 3$, then*

$$F_{kr+n}(P)=a^{kn}b^{k^2}F_n(P)\qquad\text{for all } k,n\ge 0. \tag{3}$$

(b) *If $r=2$, then*

$$\left.\begin{aligned}F_{2k}(P)&=0\\ F_{2k+1}(P)&=a^kb^{(k^2-k)/2}\end{aligned}\right\}\quad\text{for all } k\ge 0 \tag{4}$$

As an immediate corollary, we deduce the periodicity of the values of the division polynomials.

Corollary 9. *Let $P\in E(\mathbb{F})$ be as in the statement of Theorem 8. Then the sequence*

$$\bigl(F_n(P)\bigr)_{n\ge 0} \tag{5}$$

is purely periodic. More precisely, if P has order r in $E(\mathbb{F})$ and if we let $q=\#\mathbb{F}$, then the sequence (5) has period rt, where $t|q-1$ if $r\ge 3$ and $t|2q-2$ if $r=2$.

Proof of Corollary 9. We begin with the case that $r \geq 3$. Let a and b be as in Theorem 8, and let $t \geq 1$ be the smallest integer such that

$$a^t = b^{t^2} = 1.$$

In particular, t divides the least common multiple of the orders of a and b in $\mathbb{F}^*$, so t divides $q-1$. Theorem 8 tells us that

$$F_{rt+n}(P) = a^{tn} b^{t^2} F_n(P) = F_n(P) \qquad \text{for all } n \geq 0,$$

which shows that the sequence (5) is periodic and that rt is a period.

Let $\ell \geq 1$ be the smallest period, i.e., the smallest integer such that $F_{\ell+n}(P) = F_n(P)$ for all $n \geq 0$. We note that $F_n(P) = 0$ if and only if $r|n$, since P has exact order r in $E(\mathbb{F})$. From $F_{\ell+r}(P) = F_r(P) = 0$, we deduce that $r|\ell$, say $\ell = rs$. Since rt is a period and $\ell = rs$ is the smallest period, we have $s|t$, which completes the proof if $r \geq 3$. (With a bit more work, one can show that $s = t$.)

If $r = 2$, then it is easy to see from (4) that $F_n(P)$ is periodic and that the period must be even. Further we compute

$$\begin{aligned} F_{2k+1+4(q-1)}(P) &= F_{2(k+2q-2)+1}(P) \\ &= a^{k+2(q-1)} b^{(k^2-k)/2+(q-1)(2k+2(q-1)-1)} \\ &= a^k b^{(k^2-k)/2} \qquad \text{since } a^{q-1} = b^{q-1} = 1, \\ &= F_{2k+1}(P) \end{aligned}$$

Thus the period divides $4(q-1)$ and is even, so it has the form rt with $t|2q-2$. □

Proof of Theorem 8. Before starting the proof, we note that if $r|n$, then both $F_{kr+n}(P)$ and $F_n(P)$ vanish, so the desired formula (3) is vacuously true for any choice of α and β. We assume henceforth that $r \nmid n$.

Let R be a complete local ring of characteristic zero with residue field $\mathbb{F}$ (e.g., the Witt ring over $\mathbb{F}$), let K be the fraction field of R, let $\mathfrak{p}$ be the maximal ideal of R, and let $\mathcal{E}/R$ be a lift of $E/\mathbb{F}$ given by a Weierstrass equation whose reduction modulo $\mathfrak{p}$ is the Weierstrass equation of $E/\mathbb{F}$ used to normalize the division polynomials on $E/\mathbb{F}$.

The reduction map $\mathcal{E}(R) \to E(\mathbb{F})$ is surjective, so we can lift $P \in E(\mathbb{F})$ to a point in $\mathcal{E}(R)$. We would like to lift P to a torsion point of order r. If r is not divisible by the characteristic p of $\mathbb{F}$, then there is a unique such lift, which can be computed by taking any lift $Q \in \mathcal{E}(R)$ and computing the limit (see Proposition 10)

$$P' = \lim_{\substack{k\to\infty \\ p^k \equiv 1 \pmod{r}}} [p^k](Q).$$

In general, if $r = p^e r'$ with $p \nmid r'$, it suffices by the Chinese remainder theorem to lift $[p^e](P)$ and $[r'](P)$, so we are reduced to the case that r is a power of p, say $r = p^e$ with $e \ge 1$. Then it may not be possible to lift P to a torsion point in $\mathcal{E}(R)$, but it is possible to do so in a finite (ramified) extension, since we always have an exact sequence

$$0 \longrightarrow \mathcal{E}^f(\bar{R})[p^\infty] \longrightarrow \mathcal{E}(\bar{R})[p^\infty] \longrightarrow \mathcal{E}(\bar{\mathbb{F}})[p^\infty] \longrightarrow 0, \quad (6)$$

where $\mathcal{E}^f$ is the formal group of $\mathcal{E}$. (We also note that $E/\mathbb{F}$ is necessarily ordinary, since $E(\mathbb{F})$ contains the p^e-torsion point P.)

We may thus choose a finite extension K'/K with ring of integers R'/R, residue field $\mathbb{F}'/\mathbb{F}$, and maximal ideal $\mathfrak{p}'|\mathfrak{p}$ so that there is a torsion point $P' \in \mathcal{E}(R')_{\text{tors}}$ satisfying $P' \cong P \pmod{\mathfrak{p}'}$. The point P' may not be uniquely determined by P, but this will not affect our argument.

We next choose a subfield K_0' of K' that is small enough so that we can embed K_0' into $\mathbb{C}$, but large enough so that the given Weierstrass equation for $\mathcal{E}$ has coordinates in K_0' and so that $P' \in \mathcal{E}(K_0')$. Having done this, we obtain an embedding

$$\mathcal{E}(K_0') \subset \mathcal{E}(\mathbb{C}) \xleftarrow[\cong]{\Phi} \mathbb{C}/L$$

for some lattice $L \subset \mathbb{C}$. We let $P' = \Phi(\xi)$ under this identification.

Lemma 7 tells us that there is a constant $\gamma \in \mathbb{C}^*$ so that

$$F_n(\Phi(\zeta)) = \gamma^{1-n^2} \frac{\sigma(n\zeta)}{\sigma(\zeta)^{n^2}} \qquad \text{for all } \zeta \in \mathbb{C} \text{ and all } n \ge 1,$$

where to ease notation, we will omit reference to the lattice L. This allows us to compute the ratio of division functions as

$$F_{kr+n}(\Phi(\zeta)) = \frac{\sigma(kr\zeta + n\zeta)}{\sigma(n\zeta)} \cdot \big(\gamma\sigma(\zeta)\big)^{n^2-(kr+n)^2} \cdot F_n(\Phi(\zeta)), \quad (7)$$

valid for all $\zeta \in \mathbb{C}$ with $n\zeta \notin L$.

By assumption, the point $\xi \in \mathbb{C}/L$ has order r. If we identify ξ with a particular element of $\mathbb{C}$, then $r\xi \in L$. This allows us to apply the transformation formula for the σ-function (see [21, Theorem I.5.4])

$$\sigma(\zeta + \lambda) = \Psi(\lambda) e^{\eta(\lambda)(\zeta + \lambda/2)} \sigma(\zeta) \qquad \text{for all } \zeta \in \mathbb{C} \text{ and } \lambda \in L. \quad (8)$$

Here $\Psi(\lambda) \in \{\pm 1\}$ and $\eta(\lambda)$ is the quasiperiod associated to λ. More precisely, Ψ is a homomorphism $\Psi : L/2L \to \{\pm 1\}$ and η is a homomorphism $\eta : L \to \mathbb{C}$. Applying (8) with $\zeta = n\xi$ and $\lambda = kr\xi$ and

using the fact that Ψ and η are homomorphisms yields

$$\begin{aligned}\frac{\sigma(kr\xi+n\xi)}{\sigma(n\xi)} &= \Psi(kr\xi)e^{\eta(kr\xi)(n\xi+kr\xi/2)}\\ &= \Psi(r\xi)^k\left(e^{\eta(r\xi)\xi}\right)^{kn}\left(e^{\eta(r\xi)r\xi/2}\right)^{k^2}. \qquad (9)\end{aligned}$$

This is valid if $n\xi \notin L$, or equivalently, if $r \nmid n$, since ξ has exact order r in $\mathbb{C}/L$.

Now we substitute (9) into (7) with $\zeta = \xi$ to obtain

$$\begin{aligned}&F_{kr+n}(\Phi(\xi))\\ &\quad= \Psi(r\xi)^k\left(e^{\eta(r\xi)\xi}(\gamma\sigma(\xi))^{-2r}\right)^{kn}\left(e^{\eta(r\xi)r\xi/2}(\gamma\sigma(\xi))^{-r^2}\right)^{k^2}F_n(\Phi(\xi)).\end{aligned}$$

In other words, we have proven that there exist numbers $\alpha, \beta \in \mathbb{C}$, depending only on ξ and independent of k and n, so that

$$F_{kr+n}(\Phi(\xi)) = \alpha^{kn}\beta^{k^2}F_n(\Phi(\xi)) \qquad \text{for all } k,n \ge 0 \text{ with } r \nmid n.$$

(We have absorbed $\Psi(r\xi)^k = (\pm 1)^k$ into the β^{k^2} terms.)

Recall that $\xi \in \mathbb{C}/L$ corresponds to the point $P' = \Phi(\xi) \in \mathcal{E}(K_0')$, so we may equally well write this as

$$F_{kr+n}(P') = \alpha^{kn}\beta^{k^2}F_n(P') \qquad \text{for all } k,n \ge 0. \qquad (10)$$

(We drop the restriction that $r \nmid n$, since as noted earlier, the formula (10) is trivially true in this case.)

We now make the assumption that $r \ge 3$, and at the end we will briefly indicate the changes needed to deal with the case $r = 2$. We substitute $(k,n) = (1,1)$ and $(k,n) = (1,2)$ into (10) to obtain

$$F_{r+1}(P') = \alpha\beta F_1(P') = \alpha\beta \qquad \text{and} \qquad F_{r+2}(P') = \alpha^2\beta F_2(P').$$

(Note that $F_1 = 1$.) Our assumption that $r \ge 3$ implies that $F_2(P') \ne 0$, so we can solve for α and β,

$$\begin{aligned}\alpha &= \frac{F_{r+2}(P')}{F_2(P')F_{r+1}(P')} \in K(P') \subset K',\\ \beta &= \frac{F_2(P')F_{r+1}(P')^2}{F_{r+2}(P')} \in K(P') \subset K'.\end{aligned} \qquad (11)$$

Thus we may view (10) as a formula in the complete local field K', since all of the quanitities appearing in it are in K'.

We claim that α and β are actually $\mathfrak{p}'$-units in K'. This follows from the fact that for points $Q \in \mathcal{E}(R') \smallsetminus \mathcal{E}^f(R')$ and integers $n \ge 1$, we have

$$F_n(Q) \equiv 0 \pmod{\mathfrak{p}'} \qquad \text{if and only if} \qquad nQ \equiv \mathcal{O} \pmod{\mathfrak{p}'}.$$

Thus (11) shows that α and β are $\mathfrak{p}'$-units provided that

$$\begin{aligned}(r+2)P' &\not\equiv \mathcal{O} \pmod{\mathfrak{p}'},\\ (r+1)P' &\not\equiv \mathcal{O} \pmod{\mathfrak{p}'},\\ 2P' &\not\equiv \mathcal{O} \pmod{\mathfrak{p}'}.\end{aligned} \tag{12}$$

But P' modulo $\mathfrak{p}'$ has exact period $r \ge 3$, so the three conditions (12) are true.

To recapitulate, we have shown that there are $\mathfrak{p}'$-units $\alpha, \beta \in K'$ such that

$$F_{kr+n}(P') = \alpha^{kn}\beta^{k^2}F_n(P') \qquad \text{for all } k, n \ge 0. \tag{13}$$

We reduce this formula modulo $\mathfrak{p}'$ and use the fact that $P' \equiv P \pmod{\mathfrak{p}}$ (remember that we chose P' to be a lift of the point $P \in E(\mathbb{F})$) to obtain

$$F_{kr+n}(P) = a^{kn}b^{k^2}F_n(P) \qquad \text{for all } k, n \ge 0,$$

where a and b are elements of the residue field $\mathbb{F}'$ of K'. To see that $a, b \in \mathbb{F}$, we substitute $(k,n) = (1,1)$ and $(k,n) = (1,2)$ and solve for a, b (cf. (11)) to obtain

$$a = \frac{F_{r+2}(P)}{F_2(P)F_{r+1}(P)} \in \mathbb{F}, \quad b = \frac{F_2(P)F_{r+1}(P)^2}{F_{r+2}(P)} \in \mathbb{F}. \tag{14}$$

(The $F_i(P)$ values are nonzero, since $F_i(P) \equiv F_i(P') \pmod{\mathfrak{p}'}$.) This completes the proof of Theorem 8 for $r \ge 3$.

Suppose now that $r = 2$. Then it is not helpful to substitute $(k,n) = (1,2)$ into (10), since both sides are zero. So instead we substitute $(k,n) = (1,1)$ and $(k,n) = (1,3)$ to obatin

$$F_{r+1}(P') = \alpha\beta F_1(P') = \alpha\beta \qquad \text{and} \qquad F_{r+3}(P') = \alpha^3\beta F_3(P'),$$

where we know that $F_3(P') \ne 0$ since P' has order $r = 2$. We can no longer solve for α and β, but we can solve for for the quantities (cf. (11))

$$\beta^2 = \frac{F_3(P')F_{r+1}(P')^3}{F_{r+3}(P')} \quad \text{and} \quad \alpha\beta = F_{r+1}(P'). \tag{15}$$

Thus β^2 and $\alpha\beta$ are in K', and by the same argument given earlier, they are actually $\mathfrak{p}'$ units in K'. We set $n = 1$ and $r = 2$ in (13) to obtain

$$F_{2k+1}(P') = \alpha^k\beta^{k^2} = (\alpha\beta)^k(\beta^2)^{(k^2-k)/2}.$$

Reducing this formula modulo $\mathfrak{p}'$ and using the fact that $P' \bmod \mathfrak{p}'$ is equal to P, we see that there are units $a, b \in \mathbb{F}'$ (i.e., $a \equiv \alpha\beta \pmod{\mathfrak{p}'}$ and $b \equiv \beta^2 \pmod{\mathfrak{p}'}$) so that

$$F_{2k+1}(P) = a^k b^{(k^2-k)/2} \qquad \text{for all } k \ge 0.$$

Finally, putting $k = 1$ shows that $a = F_3(P) \in \mathbb{F}$ and then putting $k = 2$ shows that $b = a^{-1}F_5(P) \in \mathbb{F}$, which completes the proof of Theorem 8 for $r = 3$. □

4. The Teichmüller character

The classical *Teichimüller character* is the unique homomorphism

$$\chi : \mathbb{Z}_p^* \longrightarrow \boldsymbol{\mu}_{p-1} \quad \text{satsifying} \quad \chi(a) \cong a \pmod{p}.$$

The Teichmüller character may be constructed as $\chi(a) = \lim a^{p^k}$. It is well known how to generalize this construction to group schemes G over $\mathbb{Z}_p$ or other complete local rings.

Proposition 10. *Let $K/\mathbb{Q}_p$ be a finite extension, let R be the ring of integers of K, let $\mathfrak{p}$ be the maximal ideal of R, and let $\mathbb{F}$ be the residue field of R. Let G/R be a group scheme, and for any point $a \in G(R)$, let $\tau(a)$ denote the order of $a \bmod p$ in the special fiber $G(\mathbb{F})$. We denote by*

$$G'(R) = \bigl\{a \in G(R) : p \nmid \tau(a)\bigr\}$$

the pullback to $G(R)$ of the prime-to-p part of $G(\mathbb{F})$.

(a) *There is a unique homomorphism*

$$\chi : G'(R) \longrightarrow G(R)_{\mathrm{tors}} \quad \textit{satsifying} \quad \chi(a) \equiv a \pmod{\mathfrak{p}}. \tag{16}$$

We call χ the Teichmüller "character" *for G/R.*

(b) *Writing the gruop law in $G(R)$ multiplicatively, the* Teichmüller character *can be computed as the limit*

$$\chi(a) = \lim_{\substack{k\to\infty \\ p^k \equiv 1 \pmod{\tau(a)}}} a^{p^k}. \tag{17}$$

(c) *The order of $\chi(a)$ in $G(R)_{\mathrm{tors}}$ is exactly $\tau(a)$.*

(d) *The reduction map $G'(R)_{\mathrm{tors}} \to G'(\mathbb{F})$ is an isomorphism.*

Proof. For lack of a suitable reference, we sketch the short proof of this well-known result. We begin by proving that the limit (17) in (b) exists.

Let $G_1(R)$ be the kernel of the reduction map $G(R) \to G(\mathbb{F})$. Then $G_1(R)$ is a pro-p group. Let $q = p^e$ be the smallest power of p satisfying $q \equiv 1 \pmod{\tau(a)}$. Then $a^q \equiv a \pmod{\mathfrak{p}}$, so for $i > j$ we have

$$a^{q^i} \cdot a^{-q^j} = \bigl(a^{q^{i-j}-1}\bigr)^{q^j} \longrightarrow 1_G \qquad \text{as } i > j \to \infty.$$

This is true since $a^{q^{i-j}} \equiv a \pmod{\mathfrak{p}}$, so $a^{q^{i-j}-1} \in G_1(R)$. Thus the sequence (17) is Cauchy, so it converges.

For $a \in G'(R)$, we now define $\chi(a)$ to be the limit (17). Then

$$\chi(a) = \lim_{i\to\infty} a^{q^i} \equiv a \pmod{p} \qquad \text{and} \qquad \chi(a)^q = \chi(a).$$

In particular, $\chi(a)^{q-1} = 1_G$, so $\chi(a) \in G(R)_{\text{tors}}$. This shows that the function χ defined by the limit (17) has the desired properties (16), and it is obvious that it is a homomorphism, which proves the existence part of (a). The uniqueness is immediate from the fact that $G_1(R)$ has no prime-to-p torsion and that $\chi(a)$ has order dividing $q-1$.

Let T be the order of $\chi(a)$, so from above, $T|q-1$. In particular, T is prime to p. Further, we have

$$\chi(a)^{\tau(a)} \equiv a^{\tau(a)} \equiv 1 \pmod{\mathfrak{p}},$$

so $\chi(a)^{\tau(a)}$ is a T^{th} root of unity whose reduction modulo $\mathfrak{p}$ is 1. The formal multiplicative group $\mathbb{G}_{m,1}(R)$ has no prime-to-p torsion, so $\chi(a)^{\tau(a)} = 1$. Thus $T|\tau(a)$. Conversely, $1 = \chi(a)^T \equiv a^T \equiv 1 \pmod{\mathfrak{p}}$, so $\tau(a)|T$. Hence $T = \tau(a)$, which completes the proof of (c).

The proof of (d) is also immediate. The map $G'(R)_{\text{tors}} \to G(\mathbb{F})$ is injective, since the formal group $G_1(R)$ has no prime-to-p torsion. On the other hand, let $\alpha \in G(\mathbb{F})$ have order τ with $p \nmid \tau$. The group G is smooth over R, so we can choose an $a \in G(R)$ with $a \equiv \alpha \pmod{p}$. Then $\tau(a) = \tau$ by definition, and $\chi(a) \in G(R)_{\text{tors}}$ satisfies

$$\chi(a) \equiv a \equiv \alpha \pmod{\mathfrak{p}}.$$

This shows that the map $G'(R)_{\text{tors}} \to G'(\mathbb{F})$ is surjective, which completes the proof of (d). □

5. The Mazur-Tate p-adic sigma function

In this section we recall a construction of Mazur and Tate, and in the next section we apply their construction to prove a p-adic limit for division polynomials on elliptic curves with ordinary reduction. We set the following notation (following [12]):

K	a finite extension of $\mathbb{Q}_p$.
R	the ring of integers of K.
$\mathfrak{p}$	the maximal ideal of R.
$\mathbb{F}$	the residue field $R/\mathfrak{p}$ of K.
$\bar{R}$	the integral closure of R in an algebraic closure $\bar{K}$ of K.
E/K	an elliptic curve over K. We also fix a minimal Weierstrass equation for E/K, from which we obtain an invariant differential $\omega = dx/(2y+a_1x+a_3)$ and a uniformizer $z = -x/y$ at $\mathcal{O}$ satisfying $(\omega/dz)(\mathcal{O}) = 1$.
$\mathcal{E}/R$	the Néron model of E.

$\mathcal{E}^f$ the formal group of $\mathcal{E}$.
F_n the n-division polynomial on E, that is, the rational function $F_n \in K(E)$ satisfying Definition 1 for the given Weierstrass equation.

Remark 1. Mazur and Tate [12] define division polynomials $F_n \in K(E)$ to be the unique functions satisfying

$$(F_n) = [n]^*(\mathcal{O}) - n^2(\mathcal{O}) \quad \text{and} \quad \left(\frac{z^{n^2}F_n(z)}{[n](z)}\right)(\mathcal{O}) = \left(\frac{\omega}{dz}(\mathcal{O})\right)^{1-n^2}.$$

This agrees with our definition (1), since we have chosen z and ω compatibly to satisfy $(\omega/dz)(\mathcal{O}) = 1$.

Theorem 11 (Mazur-Tate)**.** *With the above notation and normalizations, assume that $p \geq 3$ and that $\mathcal{E}$ has good ordinary reduction. Then there is a unique power series $\sigma \in z + z^2R[[z]]$ satisfying*

$$\sigma(nQ) = \sigma(Q)^{n^2}F_n(Q) \qquad \text{for all } Q \in \mathcal{E}^f(\bar{R}). \tag{18}$$

Proof. See [12, Section 2] for the construction of σ and [12, Theorem 3.1] for a description of its properties. The construction of σ actually works as long as $\mathcal{E}$ has ordinary reduction, i.e., if $\mathcal{E}^f$ is isomorphic over $\bar{\mathbb{F}}$ to the formal multiplicative group $\mathbb{G}_m^f$. If one chooses a different Weierstrass equation for E, then F_n changes by a constant factor of the form c^{n^2-1} with $c \in R^*$, and hence σ changes by a factor c. □

Remark 2. Theorem 11 remains true for $p = 2$ provided that everything is squared. That is, there is a unique power series $\sigma^2 \in z^2 + z^3R[[z]]$ satisfying $\sigma^2(nQ) = \sigma(Q)^{2n^2}F_n^2(Q)$. But it is not possible to unambiguously take a square root and have (18) hold for all $n \geq 1$ and all $Q \in \mathcal{E}^f(\bar{R})$.

6. A p-adic limit of division polynomials

In this section we compute the p-adic limit of the values of certain subseqeunces of the division polynomials evaluated at a point. We continue with the notation from Section 5.

Theorem 12. *Assume that $p \geq 3$ and that $\mathcal{E}$ has good ordinary reduction, and let $P \in \mathcal{E}(R) \smallsetminus \mathcal{E}^f(R)$.*

(a) *There exists a power $q = p^N$ so that for every $m \geq 1$, the limit*

$$G_{m,q}(P) := \lim_{k\to\infty} F_{mq^k}(P) \quad \text{converges in } R. \tag{19}$$

(b) *$G_{m,q}(P)$ is algebraic over $\mathbb{Q}(E)$.*

(c) *In order to specify an allowable value for q, let $r \ge 2$ be the order of $P \bmod \mathfrak{p}$. Then Corollary 9 tells us that the sequence*

$$(F_n(P) \bmod \mathfrak{p})_{n\ge 0}$$

is periodic with period rt for some integer $t \ge 1$ with $p \nmid t$. Let r' be the p-free part of r, that is, $r' = rp^{-\operatorname{ord}_p(r)}$, and let $e \ge 1$ be an exponent so that

$$q = (\mathsf{N}\mathfrak{p})^e \quad \textit{satisfies} \quad q \equiv 1 \pmod{r't}.$$

Then the limit (19) in (a) exists for this value of q.

(d) *Continuing with the notation from (c), we have*

$$G_{m,q}(P)^{r'^2} \in \mathbb{Q}(\boldsymbol{\mu}(K), E[r']),$$

where $\boldsymbol{\mu}(K)$ denotes the roots of unity in K. Further,

$$G_{m,q}(P) = 0 \quad \textit{if and only if} \quad m \equiv 0 \pmod{r'}.$$

Remark 3. We note that it is quite easy to estimate the valuation of $F_n(P)$, either directly as in [2] or using the transformation formula for local height functions. In particular, with notation as in Theorem 12, it is an elementary exercise to prove that

$$v\big(F_{rn}(P)\big) = v(n) + O(1) \quad \text{for all } n \ge 1,$$

and hence $F_{rp^k}(P) \to 0$ as $k \to \infty$. Thus the interest and the depth of Theorem 12 lies in the convergence of $F_{mq^k}(P)$ in those cases that the limit is not zero.

Before starting the proof of Theorem 12, we give an elementary result that will allow us to take roots of convergent sequences.

Lemma 13. *Let $(A_k)_{k\ge 0}$ be a sequence in R^* with the property that $(A_k \bmod \mathfrak{p})_{k\ge 0}$ is constant. Let $n \ge 1$ be an integer with $p \nmid n$. Then*

$$\lim_{k\to\infty} A_k^n \textit{ exists in } R \iff \lim_{k\to\infty} A_k \textit{ exists in } R.$$

Proof. One direction is trivial. So we assume that $\lim_{k\to\infty} A_k^n$ exists and we must prove that we may take the n^{th} root. Fix $\alpha \in R^*$ with $\alpha \equiv A_k \pmod{\mathfrak{p}}$ for all $k \ge 0$. Then for any $j, k \ge 0$ we have

$$\sum_{\ell=0}^{n-1} A_j^\ell \cdot A_k^{n-1-\ell} \equiv n\alpha^{n-1} \not\equiv 0 \pmod{\mathfrak{p}},$$

from which we deduce that

$$\begin{aligned}\lim_{j,k\to\infty} |A_j - A_k| &= \lim_{j,k\to\infty} \frac{\left|A_j^n - A_k^n\right|}{\left|\sum_{\ell=0}^{n-1} A_j^\ell \cdot A_k^{n-1-\ell}\right|} \\ &= \lim_{j,k\to\infty} \left|A_j^n - A_k^n\right| \\ &= 0 \qquad \text{since } A_k^n \text{ converges as } k \to \infty.\end{aligned}$$

This shows that the sequence $(A_k)_{k\geq 0}$ is Cauchy, hence converges, in R, which completes the proof of the lemma. □

We are now ready to prove our main result.

Proof of Theorem 12. We use Lemma 6 twice to obtain

$$\big(F_r \circ [n]\big) \cdot F_n^{r^2} = F_{nr} = F_{rn} = \big(F_n \circ [r]\big) \cdot F_r^{n^2},$$

and hence

$$F_n^{r^2} = \frac{\big(F_n \circ [r]\big) \cdot F_r^{n^2}}{\big(F_r \circ [n]\big)}.$$

We evaluate this identity at the point P and use the fact that $rP \in \mathcal{E}^f(R)$ to rewrite $F_n(rP)$ using the Mazur-Tate sigma function. Thus

$$\begin{aligned}F_n(P)^{r^2} &= \frac{F_n(rP)F_r(P)^{n^2}}{F_r(nP)} \\ &= \frac{\Big(\sigma(nrP)/\sigma(rP)^{n^2}\Big)\, F_r(P)^{n^2}}{F_r(nP)} \qquad \text{from Theorem 11,} \\ &= \frac{\sigma(rnP)}{F_r(nP)} \cdot \left(\frac{F_r(P)}{\sigma(rP)}\right)^{n^2}. \qquad (20)\end{aligned}$$

We consider first the case that $p \nmid r$, so we may let $T = \chi(P) \in E[r]$ be the Teichmüller image of P (Proposition 10), and then $Q = P - T$ satisfies $Q \in \mathcal{E}^f(R)$. (See Section 4.) Note that $T \neq \mathcal{O}$, since we have assumed that $P \notin \mathcal{E}^f$. Using $rP = r(T+Q) = rQ$, we can rewrite (20) as

$$F_n(P)^{r^2} = \frac{\sigma(rnQ)}{F_r(nT+nQ)} \cdot \left(\frac{F_r(T+Q)}{\sigma(rQ)}\right)^{n^2}. \qquad (21)$$

Let

$$\tau_T : \mathcal{E} \longrightarrow \mathcal{E}$$

be the translation-by-T map. The division function F_r has simple zeros at all nonzero r-torsion points, and our assumption that $p \nmid r$ implies

that the same is true of the restriction of F_r to the special fiber of $\mathcal{E}$. Hence

$$F_r \circ \tau_T = z \cdot g_T \tag{22}$$

for a rational function $g_T \in K(E)$ whose restriction to the special fiber of $\mathcal{E}$ is regular and nonvanishing at $\mathcal{O}$, i.e., $g_T(\mathcal{O}) \in R^*$.

Then using the fact that $Q \in \mathcal{E}^f(R)$ and $p \nmid r$, we see that

$$\begin{aligned}\frac{F_r(T+Q)}{\sigma(rQ)} &= \frac{z(Q)\cdot g_T(Q)}{\sigma(rQ)} \\ &= \frac{z(Q)}{z(rQ)} \cdot \frac{z(rQ)}{\sigma(rQ)} \cdot g_T(Q) \\ &\equiv \frac{1}{r} g_T(\mathcal{O}) \pmod{\mathfrak{p}}.\end{aligned}$$

Hence if we let $n = mq^k$ with q a power of $\mathsf{N}\mathfrak{p}$ and with some fixed m and if we let $k \to \infty$, then we can evaluate the limit of the second factor in (21) as

$$\lim_{k\to\infty} \left(\frac{F_r(T+Q)}{\sigma(rQ)} \right)^{(mq^k)^2} = \chi\left(\frac{g_T(\mathcal{O})}{r} \right)^{m^2},$$

where $\chi : R^* \to \boldsymbol{\mu}(K)$ is the Teichmüller character on K (cf. Proposition 10). In particular, the value is a root of unity in K.

In order to evaluate the limit of the first factor in (21), we take a sequence of n's of the form $n = mq^k$ with $k = 1, 2, 3, \ldots$, where q is a certain fixed power of p. More precisely, we already noted that we want q to be a power of $\mathsf{N}\mathfrak{p}$, and we now further specify that

$$q = (\mathsf{N}\mathfrak{p})^e \qquad \text{satisfies} \qquad q \equiv 1 \pmod{rt}. \tag{23}$$

In particular, $q \equiv 1 \pmod{r}$, so $n \equiv m \pmod{r}$ for all k, and hence $nT = mT$ is independent of k. To ease notation, we let $Q_k = nQ = mq^kQ$, so the first factor in (21) is $\sigma(rQ_k)/F_r(mT + Q_k)$. Our task is to evaluate the limit of this fraction as $Q_k \to \mathcal{O}$. There are two cases to consider.

First, if $r|m$, then $mT = \mathcal{O}$, so we must evaluate the limit of $\sigma(rQ_k)/F_r(Q_k)$. The function $\sigma \circ [r]$ has a simple zero at $\mathcal{O}$, while F_r has a pole of order $r^2 - 1$ at $\mathcal{O}$, so $(\sigma \circ [r])/F_r$ vanishes (to order r^2) at $\mathcal{O}$. Hence in this case the limit is 0.

The more interesting case is when $r \nmid m$, so mT is a nonzero torsion point. Then

$$\begin{aligned}\frac{\sigma(rQ_k)}{F_r(mT+Q_k)} &= \frac{\sigma(rQ_k)}{z(Q_k)\cdot g_{mT}(Q_k)} \qquad \text{from (22)},\\ &= \frac{\sigma(rQ_k)}{z(rQ_k)}\cdot\frac{z(rQ_k)}{z(Q_k)}\cdot\frac{1}{g_{mT}(Q_k)}\\ &\xrightarrow[Q_k\to\mathcal{O}]{} \frac{r}{g_{mT}(\mathcal{O})}.\end{aligned}$$

To recapitulate, taking q as specified in (23), we have proven that

$$\lim_{k\to\infty} F_{mq^k}(P)^{r^2} = \begin{cases} 0 & \text{if } r|m,\\ (r/g_{mT}(\mathcal{O}))\cdot\chi(g_T(\mathcal{O})/r)^{m^2}\neq 0 & \text{if } r\nmid m.\end{cases} \tag{24}$$

This almost completes the proof when $p \nmid r$, the only difficulty being that if $r \nmid m$, then we have only computed a power of the desired limit. In order to take the r^2-root, we consider the sequence

$$A_k = F_{mq^k}(P), \qquad k = 0, 1, 2, \ldots.$$

We observe first that the sequence $A_k \bmod \mathfrak{p}$ is actually constant, since the sequence $(F_n(P) \bmod \mathfrak{p})_{n\ge 0}$ is periodic (Corollary 9) with period rt and q satisfies $q \equiv 1 \pmod{rt}$ from (23). Thus

$$mq^k \equiv m \pmod{rt} \qquad \text{for every } k \ge 0,$$

and hence

$$A_k = F_{mq^k}(P) \equiv F_m(P) = A_0 \pmod{\mathfrak{p}} \qquad \text{for all } k \ge 0.$$

On the other hand, we have already proven that $\lim_{k\to\infty} A_k^{r^2}$ exists in R. So we can apply Lemma 13 (with $n = r^2$) to the sequence A_k and deduce that $\lim_{k\to\infty} A_k$ exists in R. This completes the proof of the theorem in the case that $p \nmid r$.

Next we consider the case that $r = p^j$ is a power of p, so in particular $j \ge 1$. For each integer $k \ge 0$, let $K_k = K(E[p^{k+1}])$, let R_k be the ring of integers of K_k, let $\mathfrak{p}_k|\mathfrak{p}$ be the maximal ideal of R_k, and let $\mathbb{F}_k = R_k/\mathfrak{p}_k$ be the residue field of K_k.

We note that for any integers $m|n$, the quotient F_n/F_m is regular away from $\mathcal{O}$, since its divisor is

$$(F_n/F_m) = [m]^*\big([n/m]^*(\mathcal{O}) - (\mathcal{O})\big) - (n^2-m^2)(\mathcal{O}) \ge -(n^2-m^2)(\mathcal{O}).$$

In particular,

$$F_{p^{k+1}} = F_{p^k}\cdot f_{p^k} \tag{25}$$

for a function $f_{p^k} \in K(E)$ that is regular away from $\mathcal{O}$ and that vanishes at the points in $E[p^{k+1}] \smallsetminus E[p^k]$.

We claim that $F_{p^k}(P) \to 0$ as $k \to \infty$. Fix a point $T \in E[p^j]$ satisfying $T \equiv P \pmod{\mathfrak{p}_j}$ (cf. the exact sequence (6)) and let $k \ge j$. Then all of the points in the set

$$\bigl\{T + T' : T' \in E^f[p^{k+1}] \smallsetminus E^f[p^k]\bigr\}$$

have that property that

$$T + T' \equiv T \equiv P \pmod{\mathfrak{p}_k} \qquad \text{and} \qquad T + T' \in E[p^{k+1}] \smallsetminus E[p^k].$$

It follows that $f_k(T + T') = 0$, and hence that

$$f_k(P) \equiv f_k(T + T') = 0 \pmod{\mathfrak{p}_k}.$$

However, $f_k(P) \in K$, so $f_k(P) \equiv 0 \pmod{\mathfrak{p}}$. Now we use (25) repeatedly to deduce that

$$F_{p^k}(P) = F_{p^j}(P) \prod_{i=j}^{k-1} f_{p^i}(P) \equiv 0 \pmod{\mathfrak{p}^{k-j}} \qquad \text{for all } k \ge j.$$

Hence

$$\lim_{k\to\infty} F_{p^k}(P) = 0. \tag{26}$$

More generally, still assuming that $r = p^j$, let $m \ge 1$ be a fixed integer and write $m = m'p^\ell$ with $p \nmid m'$. Then

$$\begin{aligned}
\lim_{k\to\infty} F_{mp^k}(P) &= \lim_{k\to\infty} F_{m'p^k}(P) \\
&= \lim_{k\to\infty} F_{p^k}(m'P) F_{m'}(P)^{p^k} && \text{from Lemma 6,} \\
&= 0 && \text{from (26),}
\end{aligned}$$

since $m'P$ also has order p^j and $F_{m'}(P) \in R$. This completes the proof in the case that $r = p^j$ is a power of p.

Finally, we consider the case that $p|r$, but r is not a power of p, say $r = p^j r'$ with $j \ge 1$ and $r' \ge 2$. Notice that the point $P' = p^j P$ has exact order r' modulo $\mathfrak{p}$, where $r' \ge 2$ and $p \nmid r'$. From above, there is a power q of p so that

$$\lim_{k\to\infty} F_{mq^k}(P') \quad \text{exists,}$$

and further the limit is 0 if and only if $r'|m$. We next use Lemma 6 to write

$$F_{mq^k}(P) = F_{mp^{-j}q^k}(p^j P) F_{p^j}(P)^{(mp^{-j}q^k)^2} = F_{mp^{-j}q^k}(P') F_{p^j}(P)^{(mp^{-j}q^k)^2}.$$

Since we are going to let $k \to \infty$, we can pull off some powers of q to compensate for the p^{-j}. To simplify notation, fix an exponent ℓ so that $p^j | q^\ell$ and let $m' = mq^\ell$. Then we find that

$$\lim_{k\to\infty} F_{mq^k}(P) = \lim_{k\to\infty} F_{m'q^k}(P') F_{p^j}(P)^{(m'q^k)^2}. \tag{27}$$

The point P' has exact order r' modulo $\mathfrak{p}$, where $r' \ge 2$ and $p \nmid r'$, so from above, we know that the first term $F_{m'q^k}(P')$ in (27) has a limit in $\mathbb{Z}_p$ as $k \to \infty$, and further that the limit is 0 if and only if $r'|m$. (Note that $r'|m$ if and only if $r'|m'$, since $p \nmid r'$.) Similarly, the second term in (27) has a limit in R, since $F_{p^j}(P) \in R^*$ (where we again use the assumption that $r' \ge 2$). More precisely, the limit is a root of unity, a power of the value of the Teichmüller character $\chi(F_{p^j}(P))$. Hence the limit in (27) exists, which completes the proof of Theorem 12(a) that in all cases,

$$G_{m,q}(P) = \lim_{k\to\infty} F_{mq^k}(P) \quad \text{exists in } R.$$

However, a closer examination of the proof given above shows that we have actually completed the proof of all four parts of Theorem 12. We showed that the limit exists for the value of q specified in (c), and we showed that $G_{m,q}(P) = 0$ precisely as specified in (d). Further the value of the limit $G_{m,q}(P)^{r'^2}$ is given explicitly in terms of certain rational functions in $K(E)$ evaluated at certain points in $E[r']$, together with certain roots of unity, so $G_{m,q}(P)$ is algebraic over $\mathbb{Q}(E)$, and in fact satisfies the property described in (d). □

7. Periodicity of division polynomials modulo $\mathfrak{p}^\mu$

We continue with the notation used in Sections 5 and 6, so $K/\mathbb{Q}_p$ is a finite extension and E/K an elliptic curve. For simplicity, assume that $p \ge 3$ and that E has good reduction.

Let $P \in E(K)$ be a point whose reduction modulo $\mathfrak{p}$ has order $r \ge 2$. We proved in Corollary 9 that the sequence $(F_n(P) \bmod \mathfrak{p})$ is periodic with period rt, where $\gcd(p,t) = 1$. More precisely, in Theorem 8 we gave an explicit formula for $F_{kr+n}(P) \bmod \mathfrak{p}$ as a function of k and n. Of course, when $n = 0$, then $F_{kr}(P) \equiv 0 \pmod{\mathfrak{p}}$.

In the context of elliptic divisibility sequences, which we will study in Section 10, Shipsey [19, Theorem 3.5.4] gives a formula (when $K = \mathbb{Q}_p$) for the value of $F_{kr}(P)$ modulo p^2, and from this she immediately deduces the periodicity of the sequence $(F_{kr}(P) \bmod p^2)_{k\ge1}$. We will use the Mazur-Tate σ-function to prove a result that is both much stronger, and yet not as general, as that of Shipsey. More precisely, we will prove the periodicity of $(F_{kr}(P) \bmod \mathfrak{p}^\mu)_{k\ge1}$ for every fixed prime power $\mathfrak{p}^\mu$, but our proof will only be valid when E has good ordinary reduction.

Theorem 14. *With notation as in Section 5, assume that $p \ge 3$ and that $\mathcal{E}$ has good ordinary reduction, and let $P \in \mathcal{E}(R) \setminus \mathcal{E}^f(R)$. Further let $r \ge 2$ be the order of P mod $\mathfrak{p}$. Then for any exponent $\mu \ge 1$, the*

sequence

$$(F_{kr}(P) \bmod \mathfrak{p}^{\mu})_{k\ge 1} \quad \textit{is periodic.} \tag{28}$$

More precisely, let $e = \operatorname{ord}_{\mathfrak{p}}(p)$ *be the ramification index of* $K_{\mathfrak{p}}/\mathbb{Q}_p$ *and let* λ *be the smallest positive integer satisfying*

$$\min_{0\le i\le \lambda}\left\{(\lambda-i)e + p^i\right\} \ge \mu. \tag{29}$$

Then the sequence (28) *has period dividing* $(\mathsf{N}\mathfrak{p}-1)p^{\lambda}$.

Proof. The point rP is in the formal group $\mathcal{E}^f(R)$, so the Mazur-Tate σ-function can be evaluated at rP. This allows us to compute

$$\begin{aligned} F_{kr}(P) &= F_k(rP)F_r(P)^{k^2} && \text{from Lemma 6,}\\ &= \frac{\sigma(krP)}{\sigma(rP)^{k^2}}F_r(P)^{k^2} && \text{from Theorem 11,}\\ &= \sigma(krP)\left(\frac{F_r(P)}{\sigma(rP)}\right)^{k^2}. \end{aligned} \tag{30}$$

We claim that the second factor is a $\mathfrak{p}$-adic unit. To see this, we observe that the composition $\sigma\circ[r]$ is well-defined on the set

$$U_r = \mathcal{E}[r] + \mathcal{E}^f(\bar{R}),$$

which is a $\mathfrak{p}$-adic analytic neighborhood of the r-torsion sections of the scheme $\mathcal{E}$. Further, since σ itself has divisor $(\mathcal{O})$ in $\mathcal{E}^f(\bar{R})$, we see that the divisor of $\sigma\circ[r]$ on the set U_r is given by

$$(\sigma\circ[r])\big|_{U_r} = [r]^*(\mathcal{O}).$$

On the other hand, the function F_r has divisor

$$(F_r) = [r]^*(\mathcal{O}) - r^2(\mathcal{O}).$$

Thus

$$\left(\frac{F_r}{\sigma\circ[r]}\right)\Bigg|_{U_r} = -r^2(\mathcal{O}). \tag{31}$$

We have assumed that $r\ge 2$, which is equivalent to the assumption that $P\notin\mathcal{E}^f$, so P and $\mathcal{O}$ do not intersect on the special fiber of $\mathcal{E}$. (More formally, P and $\mathcal{O}$ determine sections $s_P, s_{\mathcal{O}} : \operatorname{Spec}(R)\to\mathcal{E}$, and our assumption ensure that the divisors $s_P(\operatorname{Spec}(R))$ and $s_{\mathcal{O}}(\operatorname{Spec}(R))$ do not intersect on the special fiber $\mathcal{E}\times_R(R/\mathfrak{p})$.) It follows from (31) that $(F_r/\sigma\circ[r])(P)$ is a $\mathfrak{p}$-adic unit.

Using this fact in (30), we have proven that there is a unit $\alpha\in R^*$ so that

$$F_{kr}(P) = \sigma(krP)\cdot\alpha^{k^2} \qquad \text{for all } k\ge 1. \tag{32}$$

The point rP is in the formal group, so we need to determine the periodicity properties of $\sigma\circ[k]$ on the formal group $\mathcal{E}^f(R)$. We use the following well-known elementary result, whose proof we briefly sketch.

Lemma 15. *Let $K/\mathbb{Q}_p$ be a finite extension with ring of integers R, maximal ideal $\mathfrak{p}$ and ramification index $e=\operatorname{ord}_{\mathfrak{p}}(p)$. Let $\mathcal{G}/R$ be a one-parameter formal group.*

(a) *For every $\lambda\ge 1$ there are power series $A_{\lambda,i}(z)\in zR[[z]]$ for $0\le i\le\lambda$ so that*

$$[p^\lambda]_{\mathcal{G}}(z)=\sum_{i=0}^{\lambda}p^{\lambda-i}A_{i,\lambda}\bigl(z^{p^i}\bigr).$$

(b) *Fix $\mu\ge 1$, and let λ be the smallest positive integer with the property that*

$$\min_{0\le i\le\lambda}\bigl\{(\lambda-i)e+p^i\bigr\}\ge\mu. \tag{33}$$

Then

$$[p^\lambda]_{\mathcal{G}}(z)\equiv 0\pmod{\mathfrak{p}^\mu}\qquad\text{for all } z\in\mathfrak{p}.$$

Equivalently, we have

$$[p^\lambda]_{\mathcal{G}}\bigl(\mathcal{G}(\mathfrak{p})\bigr)\subset\mathcal{G}(\mathfrak{p}^\mu).$$

Proof of Lemma 15. (a) The multiplication-by-p map on any formal group has the form

$$[p](z)=pF(z)+G(z^p)\qquad\text{for some } F,G\in R[[z]].$$

This is most easily proven using the invariant differential, see for example [20, Corollary IV.4.4]. This proves (a) for $\lambda=1$. The general case is then easily proven by induction, using the formula $[p^{\lambda+1}](z)=[p]\bigl([p^\lambda](z)\bigr)$.

In order to prove (b), we observe that (a) implies that

$$\operatorname{ord}_{\mathfrak{p}}\bigl([p^\lambda](z)\bigr)\ge\min_{0\le i\le\lambda}\bigl\{(\lambda-i)e+p^i\bigr\}\qquad\text{for all } z\in\mathfrak{p}.$$

Then our choice of λ to satisfy (33) yields

$$\operatorname{ord}_{\mathfrak{p}}\bigl([p^\lambda](z)\bigr)\ge\mu\qquad\text{for all } z\in\mathfrak{p}.$$

This is just another way of saying the $[p^\lambda](z)\equiv 0\pmod{\mathfrak{p}^\mu}$, which completes the proof of Lemma 15. □

We resume the proof of the theorem and we assume that λ is chosen as specified in (29), so Lemma 15 tells us that

$$[p^\lambda](Q)\equiv 0\pmod{\mathfrak{p}^\mu}\qquad\text{for all } Q\in\mathcal{E}^f(\bar{R}).$$

In particular, this is true for $Q = rP$, where P was our original point whose order modulo $\mathfrak{p}$ is r. Hence

$$[p^\lambda r](P) = [p^\lambda](rP) \equiv 0 \pmod{\mathfrak{p}^\mu},$$

so for any $k, j \ge 1$ we have

$$[(k+mp^\lambda)r](P) = [kr](P) + [m]\big([p^\lambda r](P)\big) \equiv [kr](P) \pmod{gp^\mu}. \tag{34}$$

Substituting this into (32), we find that for all $k, m \ge 1$,

$$\begin{aligned} F_{(k+mp^\lambda)r}(P) &= \sigma\big((k+mp^\lambda)rP\big) \cdot \alpha^{(k+mp^\lambda)^2} && \text{from (32)},\\ &\equiv \sigma(krP) \cdot \alpha^{(k+mp^\lambda)^2} \pmod{\mathfrak{p}^\mu} && \text{from (34)},\\ &= F_{kr}(P) \cdot \alpha^{(k+mp^\lambda)^2-k^2} && \text{from (32)},\\ &= F_{kr}(P) \cdot \big(\alpha^{2+mp^\lambda}\big)^{mp^\lambda}. \end{aligned}$$

In particular, if mp^λ is a multiple of

$$\#(R/\mathfrak{p}^\mu) = \mathsf{N}\mathfrak{p}^\mu - \mathsf{N}\mathfrak{p}^{\mu-1},$$

then $\beta^{mp^\lambda} \equiv 1 \pmod{\mathfrak{p}^\mu}$ for all $\mathfrak{p}$-adic units β. However, we observe that taking $i = 0$ in our definition (29) of λ, we have $\lambda e + 1 \ge \mu$, which implies that $\mathsf{N}\mathfrak{p}^{\mu-1}$ automatically divides p^λ. Thus it suffices to take m divisible by $\mathsf{N}\mathfrak{p} - 1$.

We have proven that if $\ell \ge 1$ is any integer satisfying

$$p^\lambda(\mathsf{N}\mathfrak{p} - 1) \,\big|\, \ell,$$

where λ is chosen to satisfy (29), then

$$F_{(k+\ell)r}(P) \equiv F_{kr}(P) \pmod{\mathfrak{p}^\mu}.$$

Hence the sequence $(F_{kr}(P) \bmod \mathfrak{p}^\mu)$ is periodic and its period is as specified in the statement of Theorem 14. □

Remark 4. For $K = \mathbb{Q}_p$, we always have

$$\min_{0\le i\le\lambda}\big\{(\lambda - i) + p^i\big\} = \lambda + 1.$$

Thus the condition (29) becomes simply $\lambda = \mu - 1$, so Theorem 14 tells us that

$$(F_{kr}(P) \bmod p^\mu)_{k\ge1} \quad \text{has period dividing } p^{\mu-1}(p-1).$$

Taking $\mu = 2$, we recover Shipsey's result, albeit in the context of division polynomials rather than elliptic divisibility sequences, and only in the case of good ordinary reduction.

Continuing with the case $K = \mathbb{Q}_p$, we consider anew the formula (32), which now says that there is an $\alpha \in \mathbb{Z}_p^*$ so that

$$F_{kr}(P) = \sigma(krP) \cdot \alpha^{k^2} \qquad \text{for all } k \geq 1. \tag{35}$$

We recall that $rP \in \mathcal{E}^f(R)$, so $z(rP) \equiv 0 \pmod{p}$. Thus

$$z(krP) = [k](z(rP)) \equiv k \cdot z(rP) \pmod{z(rP)^2},$$

so in particular, $z(krP) \equiv k \cdot z(rP) \pmod{p^2}$. Hence with our normalization of the Mazur-Tate σ-function, it follows that

$$\sigma(krP) \equiv k \cdot z(rP) \pmod{p^2}. \tag{36}$$

Applying (35) and (36) twice, once with arbitrary k and once with $k = 1$, we deduce the simple formula

$$F_{kr}(P) \equiv k \cdot \alpha^{k^2-1} \cdot F_r(P) \pmod{p^2}. \tag{37}$$

This may be compared with Shipsey's formula [19, Theorem 3.5.4] for an elliptic divisibility sequence (W_n) modulo p^2, for which she proves (under suitable hypotheses)

$$W_{kr} \equiv k \cdot \beta^{k^2-1} \cdot W_r \pmod{p^2}.$$

(We have simplified Shipsey's formula by observing that $(-1)^{k+1}$ is equal to $(-1)^{k^2-1}$, so our β is the negative of Shipsey's b.)

It is interesting to note that an analogous formula for $F_{kr}(P) \bmod p^3$ would necessarily be more complicated, since it becomes necessary to consider more than the first term of the power series for $[k](z)$ and $\sigma(z)$. On the other hand, using the fact that

$$F_{p^{\mu-1}r}(P) \equiv 0 \pmod{p^\mu},$$

it is possible to give a simple formula for the sequence

$$\left(F_{kp^{\mu-1}r}(P) \bmod p^{\mu+1}\right)_{k\geq 1}$$

that generalizes (37). We leave the details to the interested reader.

8. Elliptic divisibility sequences

We are going to use Theorem 12 to partially prove a conjecture concerning the p-adic behavior of classical elliptic divisibility sequences. Our inspiration for this result, and indeed the original motivation for much of the work in this paper, is aptly summarized by the following quote from Morgan Ward's monograph [24, page 33].

> If the least positive residues modulo m of the successive values $U_0, U_1, U_2, \dots$ of any Lucas function (i.e., $U_n = (\alpha^n - \beta^n)/(\alpha - \beta)$) are calculated, the pattern of residues exhibits interesting symmetries. These symmetries extend to elliptic sequences, and find their ultimate explanation in the periodicity of the second kind of the Weierstrass sigma function.

We recall the general definition of a *divisibility sequence* as being a sequence of integers $(D_n)_{n\ge 0}$ satisfying

$$m|n \Longrightarrow D_m|D_n.$$

A standard example of a divisibility sequence is one of the form $a^n - 1$, and more generally, divisibility sequences may appear as linear recurrence sequences such as the Fibonacci sequence. A complete classification of divisibility sequences associated to linear recurrences is given in [1].

It is less clear that there are interesting divisibility sequences satisfying nonlinear recurrences. The most famous examples of such sequences are associated to the recursion formula for division polynomials on elliptic curves.

Definition 2. An *elliptic divisibility sequence* (abbreviated EDS) is a divisibility sequence $\mathcal{W} = (W_n)_{n\ge 0}$ satisfying the formula

$$W_{m+n}W_{m-n} = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2 \qquad \text{for all } m \ge n \ge 1. \quad (38)$$

The arithmetic properties of elliptic divisibility sequences were first studied in detail by Morgan Ward [24, 25] in the 1940's, and recently there has been a resurgence of interest in their study [3, 4, 5, 8, 9, 10, 19, 23, 22]. (See also [11, 13, 14] for work on the related Somos sequences.) Ward calls an EDS *proper* if

$$W_0 = 0, \qquad W_1 = 1, \qquad \text{and} \qquad W_2W_3 \ne 0,$$

and he proves that a proper EDS is associated to a pair $(E_{\mathcal{W}}, P_{\mathcal{W}})$ consisting of a (possibly singular) elliptic curve and a rational point $P_{\mathcal{W}} \in E_{\mathcal{W}}(\mathbb{Q})$. Further, the sequence $\mathcal{W}$ satisfies a linear recurrence if and only if the curve $E_{\mathcal{W}}$ is singular and is bounded if and only if $P_{\mathcal{W}}$ is a torsion point.

Remark 5. The nonsingularity of the curve $E_{\mathcal{W}}$ associated to a proper elliptic divisibility sequence $\mathcal{W}$ is equivalent to the nonvanishing of the

discriminant

$$\begin{aligned}\mathrm{Disc}(\mathcal{W}) = W_4W_2^{15} - W_3^3W_2^{12} + 3W_4^2W_2^{10} - 20W_4W_3^3W_2^7 \\ + 3W_4^3W_2^5 + 16W_3^6W_2^4 + 8W_4^2W_3^3W_2^2 + W_4^4. \quad (39)\end{aligned}$$

This is essentially the discriminant of the curve $E_{\mathcal{W}}$ (cf. Ward [24, equation (19.3)]). See [24] or [22, Appendix] for additional formulas describing $E_{\mathcal{W}}$ and $P_{\mathcal{W}}$.

Remark 6. Except in some degenerate cases, the definition of an EDS forces $W_0 = 0$ (put $m = n$ in (38)) and $W_1 = \pm 1$ (put $n = 1$). As noted above, a proper EDS with $\mathrm{Disc}(\mathcal{W}) = 0$ satisfies a linear recurrence. See [19, 24] for details and a complete description of nonproper EDS.

Definition 3. We call $\mathcal{W}$ a *general elliptic divisibility sequences* if it satisfies:

(1) $\mathcal{W}$ is proper;
(2) $E_{\mathcal{W}}$ is a nonsingular elliptic curve, or equivalently, $\mathrm{Disc}(\mathcal{W}) \neq 0$;
(3) $P_{\mathcal{W}}$ is a point of infinite order in $E_{\mathcal{W}}(\mathbb{Q})$, or equivalently, $\mathcal{W}$ is unbounded.

From our earlier remarks, these are the most interesting EDS. (Note that this definition differs somewhat from Ward's terminology.)

Example 1. The simplest general elliptic divisibility sequence is the sequence

$$\begin{aligned}1, 1, -1, 1, 2, -1, -3, -5, 7, -4, -23, 29, 59, 129, -314, \\ - 65, 1529, -3689, -8209, -16264, \ldots \quad (40)\end{aligned}$$

It is associated to the generator $P = (0, 0)$ of the Mordell-Weil group on the elliptic curve $y^2 + y = x^3 - x$ of conductor 37.

An elliptic divisibility sequence (W_n) is required to satisfy the recursion (38) for all $m \geq n \geq 1$. It is easy to check that it suffices that (W_n) satisfy the two relations

$$W_{2n+1} = W_{n+2}W_n^3 - W_{n-1}W_{n+1}^3, \quad (41)$$

$$W_{2n}W_2 = W_n\left(W_{n+2}W_{n-1}^2 - W_{n-2}W_{n+1}^2\right). \quad (42)$$

In particular, a proper EDS is determined by the values of W_2, W_3, W_4. Further, a triple W_2, W_3, W_4 with $W_2W_3 \neq 0$ gives an EDS if and only if $W_2 | W_4$. (See [24].) Additional material on elliptic divisibility sequences may be found in [4, 5, 8, 9, 10, 19, 23, 22, 24, 25].

9. Elliptic divisibility sequences and elliptic functions

We recall Ward's fundamental result relating elliptic divisibility sequences to values of elliptic functions.

Theorem 16. *Let (W_n) be a general elliptic divisibility sequence. Then there is a lattice $L \subset \mathbb{C}$ and a complex number $\xi \in \mathbb{C}$ such that*

$$W_n = \psi_n(\xi, L) = \frac{\sigma(n\xi, L)}{\sigma(\xi, L)^{n^2}} \qquad \text{for all } n \ge 1,$$

where $\psi_n(\xi, L)$ and $\sigma(\xi, L)$ are, respectively, the (analytic) n-division polynomial and the Weierstrass σ-function associated to the lattice L.

Further, the modular invariants $g_2(L)$ and $g_3(L)$ associated to the lattice L and the Weierstrass values $\wp(\xi, L)$ and $\wp'(\xi, L)$ associated to the point ξ on the elliptic curve $\mathbb{C}/L$ are in the field $\mathbb{Q}$. (More precisely, $g_2(L), g_3(L), \wp(\xi, L), \wp'(\xi, L)$ are given as rational expressions in $\mathbb{Q}(W_2, W_3, W_4)$.)

Proof. See Ward [24, Theorems 12.1 and 19.1]. The rational expressions for g_2 and g_3 in $\mathbb{Q}(W_2, W_3, W_4)$ are given by [24, equations 13.6 and 13.7], and the rational expressions for $\wp(\xi, L)$ and $\wp'(\xi, L)$ are given by [24, equations 13.5 and 13.1]. See also [22, Appendix] for simplified formulas. □

We also mention that Ward proves a partial converse to Theorem 16.

Theorem 17. *Let L be a lattice with $g_2(L), g_3(L) \in \mathbb{Q}$ and let $\xi \in \mathbb{C}$ satisfy $\wp(\xi, L), \wp'(\xi, L) \in \mathbb{Q}$. Then there is a constant $c \in \mathbb{Q}^*$ so that the sequence $(c^{n^2-1}\psi_n(\xi, L))$ is an elliptic divisibility sequence.*

Proof. This is proven in [24, Theorem 21.4]. See also [19, 23]. □

We reformulate Ward's result so that it is entirely in terms of rational numbers.

Proposition 18. *Let $\mathcal{W} = (W_n)$ be a nonsingular elliptic divisibility sequence, and let $E_{\mathcal{W}}/\mathbb{Q}$ and $P_{\mathcal{W}} \in E(\mathbb{Q})$ be the associated elliptic curve and rational point. Fix a minimal Weierstrass equation for $E_{\mathcal{W}}$, and let F_n be the normalized n-division polynomial on $E_{\mathcal{W}}$ (Definition 1). Then there is a constant $\gamma \in \mathbb{Q}^*$ so that*

$$W_n = \gamma^{n^2-1} F_n(P_{\mathcal{W}}) \qquad \text{for all } n \ge 1.$$

Further, the denominator of γ is divisible only by primes of bad reduction of $P_{\mathcal{W}}$, i.e., primes p of bad reduction for $E_{\mathcal{W}}$ at which $P_{\mathcal{W}} \bmod p$ is the singular point on $E_{\mathcal{W}} \bmod p$.

Proof. We use Theorem 16 to choose a lattice L and complex number $\xi \in \mathbb{C}$ so that the given EDS has the form $W_n = \psi_n(\xi, L)$ for all $n \ge 1$. Let $\Phi : \mathbb{C}/L \to E(\mathbb{C})$ be an isomorphism. Then Lemma 7 tells us that there is a constant $\gamma \in \mathbb{C}^*$ so that

$$F_n(\Phi(\zeta)) = \gamma^{1-n^2}\psi_n(\zeta, L) \qquad \text{for all } \zeta \in \mathbb{C} \text{ and all } n \ge 1.$$

Substituting $\zeta = \xi$, so $P_{\mathcal{W}} = \Phi(\xi)$, we obtain

$$F_n(P_{\mathcal{W}}) = \gamma^{1-n^2}\psi_n(\xi, L) = \gamma^{1-n^2}W_n \qquad \text{for all } n \ge 1.$$

Putting $n = 2$ and $n = 3$, we find that γ^3 and γ^8 are in $\mathbb{Q}$, and hence that $\gamma \in \mathbb{Q}$, which completes the proof that $W_n = \gamma^{n^2-1}F_n(P_{\mathcal{W}})$ with $\gamma \in \mathbb{Q}^*$.

Since $W_n \in \mathbb{Z}$, we see that

$$\begin{aligned}\operatorname{ord}_p(F_n(P_{\mathcal{W}})) &= \operatorname{ord}_p W_n - (n^2-1)\operatorname{ord}_p(\gamma) \\ &\ge -(n^2-1)\operatorname{ord}_p(\gamma) \qquad \text{for all } n \ge 1. \end{aligned} \tag{43}$$

Let p be a prime such that $P_{\mathcal{W}} \bmod p$ is nonsingular. Then $P_{\mathcal{W}} \bmod p$ cannot have order both 2 and 3, so at least one of $F_2(P_{\mathcal{W}})$ and $F_3(P_{\mathcal{W}})$ is nonzero modulo p. Then (43) says that either

$$0 = \operatorname{ord}_p(F_2(P_{\mathcal{W}})) \ge -3\operatorname{ord}_p(\gamma) \text{ or } 0 = \operatorname{ord}_p(F_3(P_{\mathcal{W}})) \ge -3\operatorname{ord}_p(\gamma),$$

and hence $\operatorname{ord}_p(\gamma) \ge 0$. □

10. A p-adic limit of elliptic divisibility sequences

In this section we apply our results on division polynomials to partially prove the following conjecture about elliptic divisibility sequences.

Conjecture 19. *Let $\mathcal{W} = (W_n)_{n\ge 0}$ be an elliptic divisibility sequence and let p be a prime. Then there is an exponent $N = N_p \ge 1$ so that for every $m \ge 1$, the limit*

$$\lim_{k\to\infty} W_{mp^{kN}}$$

converges in $\mathbb{Z}_p$ to a number that is algebraic over $\mathbb{Q}$.

We are able to prove this conjecture for "most" elliptic divisibility sequences and for "most" primes.

Theorem 20. *Let $\mathcal{W} = (W_n)_{n\ge 0}$ be a general elliptic divisibility sequence. Let $E_{\mathcal{W}}$ be the associated elliptic curve, given by a minimal Weierstrass equation over $\mathbb{Q}$, let $P_{\mathcal{W}} \in E_{\mathcal{W}}(\mathbb{Q})$ be the associated rational point, and let $S_{\mathcal{W}}$ be the set of primes p satisfying any one of the following conditions:*

- $p = 2$.
- $P_{\mathcal{W}} \equiv \mathcal{O} \pmod{p}$.
- $P_{\mathcal{W}} \bmod p$ *is a singular point on* $E_{\mathcal{W}} \bmod p$.
- $E_{\mathcal{W}} \bmod p$ *is supersingular.*

Then Conjecture 19 is true for $\mathcal{W}$ *for all primes* $p \notin S_{\mathcal{W}}$*, that is, there is an exponent* $N = N_p \ge 1$ *so that for every* $m \ge 1$*, the limit*

$$\lim_{k\to\infty} W_{mp^{kN}}$$

converges in $\mathbb{Z}_p$ *to a number that is algebraic over* $\mathbb{Q}$.

In particular, if $E_{\mathcal{W}}$ *does not have complex multiplication, then Conjecture 19 is true for almost all primes in the sense of density, since* $S_{\mathcal{W}}$ *has density* 0. (*If* $E_{\mathcal{W}}$ *has CM, then* $S_{\mathcal{W}}$ *has density* $\frac{1}{2}$.)

Proof. We use Proposition 18 to find a $\gamma \in \mathbb{Q}^*$ so that

$$W_n = \gamma^{n^2-1} F_n(P_{\mathcal{W}}) \qquad \text{for all } n \ge 1. \tag{44}$$

Proposition 18 also tells us that $\operatorname{ord}_p(\gamma) \ge 0$, since we have assumed that $P_{\mathcal{W}} \bmod p$ is nonsingular. On the other hand, our assumption that $P_{\mathcal{W}} \not\equiv \mathcal{O} \pmod{p}$ implies that $\operatorname{ord}_p(F_n(P_{\mathcal{W}})) \ge 0$, so if $\operatorname{ord}_p(\gamma) > 0$, then

$$\operatorname{ord}_p(W_n) \ge (n^2-1)\operatorname{ord}_p(\gamma) \longrightarrow \infty \quad \text{as } n \to \infty.$$

Thus if $\operatorname{ord}_p(\gamma) > 0$, then $\lim_{n\to\infty} W_n = 0$ in $\mathbb{Z}_p$.

We are thus reduced to the case that $\gamma \in \mathbb{Z}_p^*$. Then for any $m \ge 1$,

$$\lim_{k\to\infty} \gamma^{mp^k-1} = \chi(\gamma)^m \gamma^{-1} \quad \text{in } \mathbb{Z}_p,$$

where $\chi(\gamma) \in \boldsymbol{\mu}_{p-1}$ is the value of the Teichmüller character. Using (44), it thus suffices to prove there is a power $q = p^N$ so that for every $m \ge 1$,

$$\lim_{k\to\infty} F_{mq^k}(P_{\mathcal{W}}) \quad \text{converges in } \mathbb{Z}_p$$

and is algebraic over $\mathbb{Q}$. This follows immediately from Theorem 12, since our choice of the set $S_{\mathcal{W}}$ was designed to ensure that Theorem 12 is applicable to every prime $p \notin S_{\mathcal{W}}$.

This completes the proof of Theorem 20 except for the final statements about densities. We note that the first three conditions specifying primes in $S_{\mathcal{W}}$ only include finitely many primes. The fourth condition, that $E_{\mathcal{W}} \pmod{p}$ be supersingular, is more serious. However, Serre [17] has proven that for any fixed non-CM elliptic curve $E/\mathbb{Q}$, almost all primes give ordinary reduction. (More precisely, the number of supersingular primes less than X is $O(X^{3/4})$, see [7, 18].) On the other hand, Elkies has shown that there are infinitely many primes of supersingular reduction [6], so unfortunately our set $S_{\mathcal{W}}$ is always

infinite. Finally, it is well known that an elliptic curve with CM has supersingular reduction at precisely the primes that are inert in its CM field. □

Remark 7. Theorem 12 tells us when the limit in Theorem 20 is nonzero. Let r_p be the order of $P_{\mathcal{W}}$ in $E_{\mathcal{W}}(\mathbb{F}_p)$, and let $q = p^N$ be the power of p in Theorem 20. Note that Hasse's theorem [20, V.1.1] implies that $r_p \leq (\sqrt{p}+1)^2$, so in particular, $r_p < p^2$ under our assumption that $p \neq 2$.

Writing $W_n = \gamma^{n^2-1} F_n(P_{\mathcal{W}})$ as in (44), we see that if $p|\gamma$, then $p|W_n$ for all $n \geq 2$, in which case $W_n \to 0$ in $\mathbb{Z}_p$. On the other hand, if $p \nmid \gamma$, then Theorem 12 implies that the limit in Theorem 20 is zero if and only if the p-free part of r_p divides m Hence

$$\lim_{k\to\infty} W_{mp^{kN}} = 0 \quad \text{if and only if either} \quad \begin{cases} p|W_n \text{ for all } n \geq 2, \text{ or} \\ r_p|mp. \end{cases}$$

Acknowledgements. The author would like to thank Noam Elkies, Graham Everest, Barry Mazur, Rachel Shipsey, Nelson Stephens, and Thomas Ward for helpful correspondence during the preparation of this paper.

References

[1] J.P. Bézivin, A. Pethö, A.J. van der Poorten, A full characterization of divisibility sequences, *Amer. J. of Math.* **112** (1990), 985–1001.

[2] J. Cheon, S. Hahn, Explicit valuations of division polynomials of an elliptic curve, *Manuscripta Math.* **97** (1998), 319–328.

[3] D.V. Chudnovsky, G.V. Chudnovsky, Sequences of numbers generated by addition in formal groups and new primality and factorization tests, *Advances in Applied Mathematics* **7** (1986), 385–434.

[4] L.K. Durst, The apparition problem for equianharmonic divisibility, Proc. Nat. Acad. Sci. U. S. A. **38** (1952), 330–333.

[5] M. Einsiedler, G. Everest, T. Ward, Primes in elliptic divisibility sequences, *LMS J. Comput. Math.* **4** (2001), 1–13, electronic.

[6] N. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$, *Invent. Math.* **89**, (1987), 561–567.

[7] ———Distribution of supersingular primes, Journées Arithmétiques, 1989 (Luminy, 1989), *Astérisque* **198-200** (1991), 127–132 (1992).

[8] G. Everest, A. van der Poorten, I. Shparlinski, T. Ward, *Recurrence sequences*, Mathematical Surveys and Monographs 104, AMS, Providence, RI, 2003.

[9] G. Everest, T. Ward, Primes in divisibility sequences, *Cubo Mat. Educ.* **3** (2001), 245–259.

[10] ———The canonical height of an algebraic point on an elliptic curve, *New York J. Math.* 6 (2000), 331-342, (electronic).

[11] D. Gale, The Strange and Surprising Saga of the Somos Sequences, *Mathematical Intelligencer* **13**, (1991) 40–42, 49–50

[12] B. Mazur, J. Tate, The p-adic sigma function, *Duke Math. J.* **62** (1991), 663–688.

[13] J. Propp, The Somos Sequence Site, `http://www.math.wisc.edu/~propp/somos.html`.

[14] R. Robinson, Periodicity of Somos sequences, *Proc. Amer. Math. Soc.* **116** (1992), 613–619.

[15] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.* **44** (1985), 483–494.

[16] ———Counting points on elliptic curves over finite fields, Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993), *J. Théor. Nombres Bordeaux* **7** (1995), 219–254.

[17] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[18] ———Quelques applications du théorème de densité de Chebotarev, *Inst. Hautes Études Sci. Publ. Math.*, **54** (1981), 323–401.

[19] R. Shipsey, Elliptic divisibility sequences, Ph.D. thesis, Goldsmith's College (University of London), 2000.

[20] J.H. Silverman, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, New York, 1986.

[21] ——— *Advanced topics in the arithmetic of elliptic curves*, GTM 151, Springer-Verlag, New York, 1994.

[22] J.H. Silverman, N. Stephens, The sign of an elliptic divisibility sequence, preprint 2004, (arXiv:mathNT/0402415).

[23] C.S. Swart, Elliptic divisibility sequences, Ph.D. thesis, Royal Holloway (University of London), 2003.

[24] M. Ward, Memoir on elliptic divisibility sequences, *Amer. J. Math.* **70** (1948), 31–74.

[25] M. Ward, The law of repetition of primes in an elliptic divisibility sequence, *Duke Math. J.* **15** (1948), 941–946.

[26] E.T. Whittaker, G.N. Watson, *A course in modern analysis*, Cambridge Univ. Press, Cambridge, 4th ed., 1927.

Mathematics Department, Box 1917, Brown University, Providence, RI 02912 USA

E-mail address: `jhs@math.brown.edu`